

Deepfake Vishing

Stopping a Voice-Cloned CEO in 20 Minutes

October 2026

forvis mazars

Today’s Presenters

Zach Shelton, CISA, CDPSE

Principal | IT Risk & Compliance

- 19 years with Forvis Mazars
- Focus areas:
  - IT Consulting / Compliance
  - Cybersecurity Consulting
  - IT Audit / SOX
  - AI Governance / Use Case Development
  - AI Voice Cloning (Deepfake) Assessments



© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Today’s Presenters

Ariana Curtis, Sec+, OSCC

Consultant | IT Risk & Compliance

- Joined Forvis Mazars in 2022
- Focus areas:
  - IT Risk & Compliance Consulting
  - Cybersecurity Consulting
  - AI Voice Cloning (Deepfake) Assessments
  - Physical Social Engineering Assessments
  - Penetration Testing / Ethical Hacking



© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Agenda

1. Setting the Scene
2. Tabletop Scenario
3. The First 20 Minutes
4. Cross-Functional Escalation
5. Key Takeaways & Discussion



© 2026 Forvis Mazars, LLP. All rights reserved.

Setting the Scene
Why This Topic Matters Now

Deepfake vishing (voice phishing) has rapidly evolved into a highly coordinated enterprise threat, marked by “channel-hopping” campaigns and a collapse in the technical barriers required to execute real-time audio clones.



Risks of Cyber Fraud

73%

report cyber-enabled fraud in their network.

The World Economic Forum now ranks AI-fueled fraud above ransomware as the top concern for corporate CEOs.

© 2026 Forvis Mazars, LLP. All rights reserved.

Setting the Scene
Deepfakes Target a Gap in Defenses

62%

Hit by a live deepfake

Organizations experienced a verified, operational deepfake incident in the prior 12 months.

41%

Audio-call attacks

Security leaders handled a deepfake on a voice call paired with a social-engineering loop; 35% faced video.

10%

The detection gap

One in 10 security executives include deepfake detection in identity-awareness programs today.

48%

Bypass corporate filters

AI-generated impersonation attempts slip past existing email and telephony security controls.

Gartner named it a top-4 threat where attackers have the upper hand.

For 2026–2027, Gartner lists identity impersonation with deepfakes alongside AI-application compromise, software supply chain attacks, and prompt injection. It maps directly to MITRE ATT&CK T1654 (voice phishing) and is used to defeat liveness checks and run CEO-fraud scams.

Sources: Gartner 2026 CISO Report; World Economic Forum Global Cybersecurity Outlook; TechRadar impersonation-bypass evaluation.
© 2026 Forvis Mazars, LLP. All rights reserved.

6–12 months

The Defender’s Window

Recorded Future’s warning on how long teams have before AI attackers overwhelm them.

“We basically have six to 12 months before defenders are going to be absolutely overwhelmed.”

– Levi Gundert, Chief Security & Intelligence Officer, Recorded Future (Mastercard Black Hat 2026 dispatch)

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Tabletop Scenario
The Voice-Cloned CEO Call

Realistic Scenario Setup

A phone call mimics the CEO's voice with urgent payment instructions and credible business context.

Time-Sensitive Decision Making

Teams face tight timing to decide whether to proceed, pause, verify, or escalate the request.

Focus on Process Over Tech

The goal is disciplined decision making under pressure, not technical detection of voice fakes.

Team Interaction & Breakdown Points

Scenario explores team interactions in the first 20 minutes and potential breakdowns in communication.

© 2026 Forvis Mazars, LLP. All rights reserved.



Tabletop Scenario

Deepfake Vishing Demo

© 2026 Forvis Mazars, LLP. All rights reserved.

Tabletop Scenario

What Success Looks Like in the First 20 Minutes

Verify

Before Acting

Slowing decisions allows time to verify requests and prevent premature actions.

Escalate

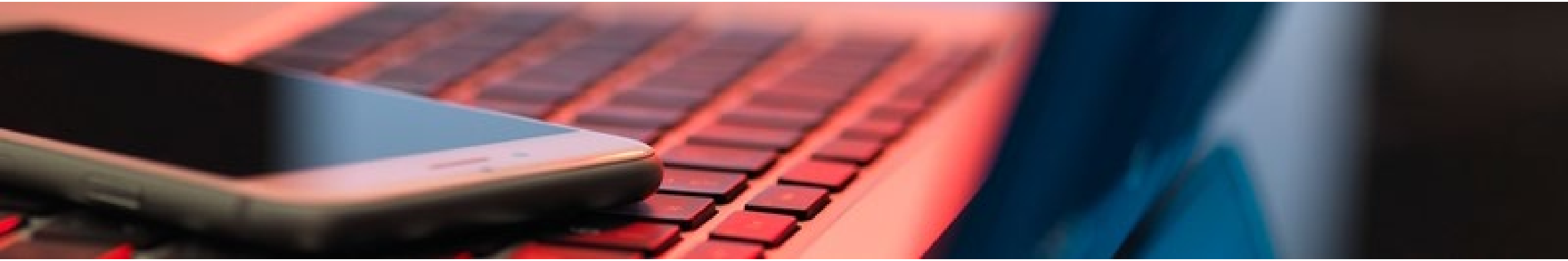
Strategically

Appropriate escalation across departments helps ensure a thorough response and risk mitigation.

Communicate

With Precision

Preparing clear internal notes can inform leadership decisions and support important communications.



© 2026 Forvis Mazars, LLP. All rights reserved.

The First 20 Minutes
Step-by-Step

Initial Response & Red Flags

Recognize red flags and pause action within the first five minutes to help prevent escalation of the deepfake vishing incident.

Decision & Communication

Document decisions and communicate internally by the 20-minute mark to help provide a coordinated and informed response.

Verification & Escalation

Perform independent identity verification and escalate to finance, IT/security, and legal teams between five to 15 minutes.

Flexible & Practical Model

The timeline is a best practice guide; IT/security leaders should validate timings and roles to reduce delays and risks.

© 2026 Forvis Mazars, LLP. All rights reserved.

The First 20 Minutes
Signals That Can Help Stop the Process



Urgency & Secrecy

Urgency combined with secrecy is a critical warning sign that requires stopping the process immediately.

Bypassing Approval Steps

Requests to bypass normal approval processes indicate potential fraud and signal to halt actions.

Changes to Payment Details

Unexpected changes to vendor or payment details are strong indicators of risk requiring immediate attention.

Pressure to Use Alternate Platforms

Pressure to move conversations to personal devices or different platforms signals a high-risk situation.

© 2026 Forvis Mazars, LLP. All rights reserved.

The First 20 Minutes
Trust But Verify Invariably



Verification Outside Origin Channel

Verification should occur outside the original channel using trusted contacts, not caller-provided information.

Dual Approval for Payment Changes

Require dual approval for payment changes to promote security and reduce the risk of fraud.

Validation of Business Context

Business context should be validated with the appropriate owner before proceeding with requests.

Documentation & SME Validation

Decisions should be documented and control implementations validated by subject matter experts (SMEs).

© 2026 Forvis Mazars, LLP. All rights reserved.

Cross-Functional Escalation
Coordinating the Organizational Response



Cross-Functional Challenge

Responding to deepfake vishing requires coordination across multiple teams, not IT alone, to act effectively within the first 20 minutes.

Defined Team Roles

Each team has a clear role: the service desk pauses the action, finance holds the payment, IT security assesses compromise, legal evaluates reporting obligations, and communications prepares employee guidance.

Importance of Escalation Paths

Predefined escalation paths and a shared understanding of the process enable a quick, coordinated response.

Cybersecurity & Governance

Cybersecurity intersects with operations, risk management, and governance, so the response must be managed holistically.

© 2026 Forvis Mazars, LLP. All rights reserved.

Cross-Functional Escalation
The First Internal Note

Do:

- State what is known and what remains unknown
- Keep the message concise, factual, and timestamped
- Provide clear instructions on immediate next steps
- Designate a single channel for questions and reporting

Don’t:

- Speculate about the source or attacker
- Assign blame to an individual or team
- Issue vague or open-ended guidance
- Distribute the message without legal and compliance review



© 2026 Forvis Mazars, LLP. All rights reserved.

Cross-Functional Escalation
What You Can Improve Starting Tomorrow

Callback Protocols

Implement callback protocols for executive and finance requests to verify authenticity and prevent fraud.

Dual Approval Processes

Require dual approval for payments or changes to bank details to strengthen financial controls.

Strict No-Exception Rules

Establish documented escalation procedures for urgent off-channel requests to help reduce social-engineering risk.

Clear Reporting & Drills

Create clear reporting paths for suspected impersonation and conduct tabletop exercises for high-risk teams.



© 2026 Forvis Mazars, LLP. All rights reserved.

Cross-Functional Escalation
Building Resilience

Long-Term Fraud Risk Management

Focus on a sustained program managing deepfake-enabled fraud risks beyond immediate controls.

Scenario-Based Training

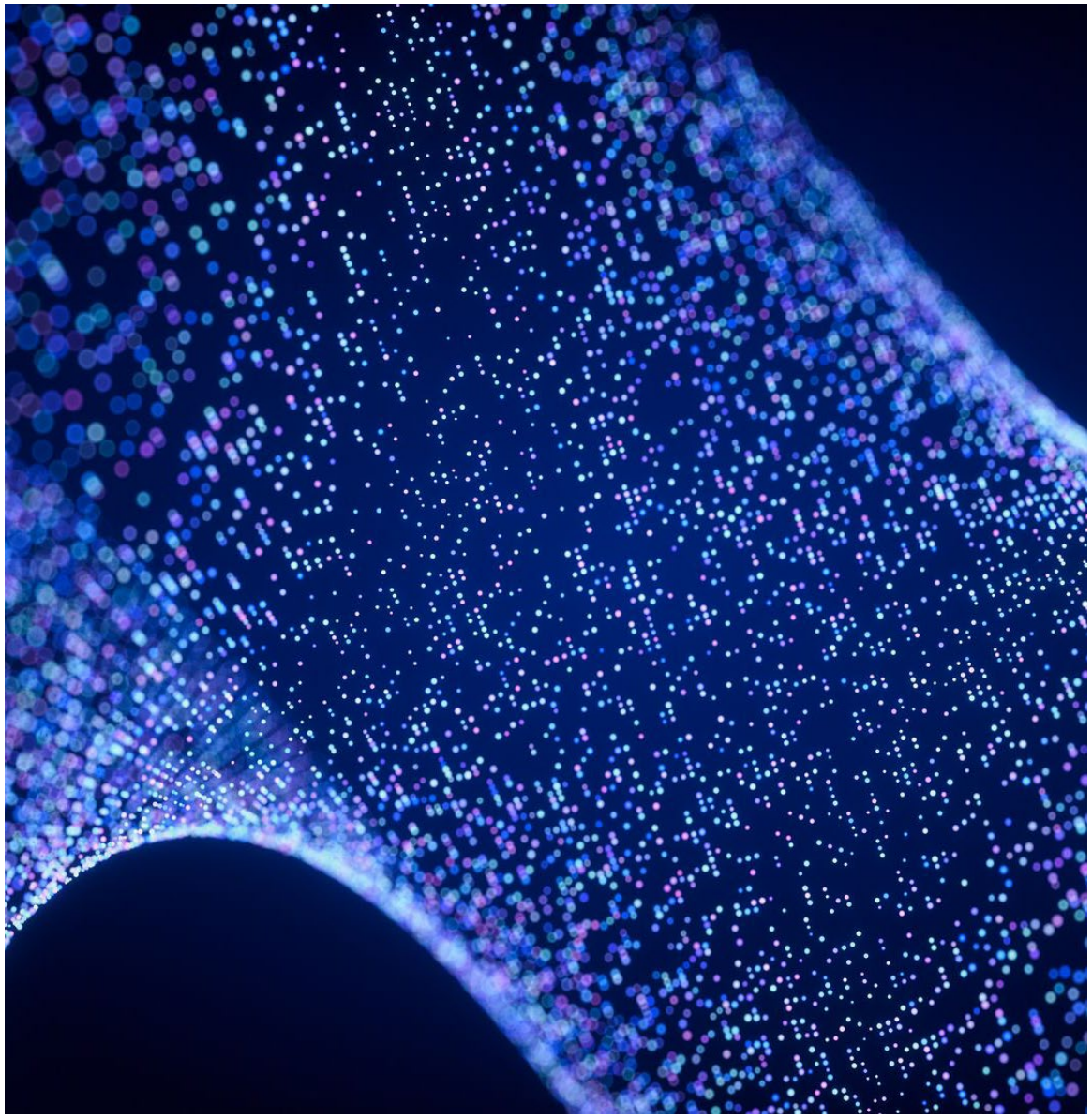
Use scenario-based exercises to help teams prepare for deepfake fraud incidents and response.

Executive Exposure Review

Assess voice and video vulnerabilities of executives with skilled validation to reduce risks.

Incident Response & Metrics

Maintain playbooks and track metrics to help improve the effectiveness of fraud incident responses.



© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Cross-Functional Escalation
Where Many Orgs Stumble

Overreliance on Voice Recognition

Organizations often trust voice recognition alone, which can be fooled by deepfake technology, elevating the risk of security breaches.

Compromised Verification Channels

Verifying requests through the same channel may be compromised, leading to insufficient authentication.

Ignoring Established Controls

Urgency may lead teams to bypass security controls, increasing vulnerability during deepfake vishing incidents.

Delaying Incident Escalation

Failing to promptly escalate suspicious activity delays response and can worsen potential impact.

© 2026 Forvis Mazars, LLP. All rights reserved.

Key Takeaways
What Leaders Should Remember

Four moves to make: pause, verify, escalate, and rehearse.

Pause High-Risk Requests

Leaders should be vigilant in pausing high-risk requests to help prevent potential issues before escalation.

Verify Through Channels

Verification through independent and trusted channels is crucial for maintaining security and accuracy.

Escalate & Communicate

Clear communication and cross-functional escalation can help support organizational alignment and a swift response.

Reusable Tabletop Exercises

Transform tabletop exercises into reusable kits for ongoing organizational preparedness and learning.

© 2026 Forvis Mazars, LLP. All rights reserved.



IT Risk & Compliance

Questions?

© 2026 Forvis Mazars, LLP. All rights reserved.



Don’t Miss the Last Session of the

2026 Cybersecurity Virtual Symposium

ERP Security: Protecting an Expanding Attack Surface

Today at 11:15 a.m. - 12:15 p.m. ET

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Contact

Forvis Mazars

Zach Shelton
Principal, IT Risk & Compliance
P: 919.301.6708
zach.shelton@us.forvismazars.com

Ariana Curtis
Consultant, IT Risk & Compliance
P: 704.367.7020
ariana.curtis@us.forvismazars.com

The information set forth in this presentation contains the analysis and conclusions of the author(s) based upon his/her/their research and analysis of industry information and legal authorities. Such analysis and conclusions should not be deemed opinions or conclusions by Forvis Mazars or the author(s) as to any individual situation as situations are fact-specific. The reader should perform their own analysis and form their own conclusions regarding any specific situation. Further, the author(s)' conclusions may be revised without notice with or without changes in industry information and legal authorities.

© 2026 Forvis Mazars, LLP. All rights reserved.